09/402144 50 CO

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GR 97 P 1472 P	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DE98/00563	International filing date (*day/month/year*) 25 February 1998 (25.02.1998)	Priority date (*day/month/year*) 14 April 1997 (14.04.1997)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 6 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
26 August 1998 (26.08.1998)	12 July 1999 (12.07.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer Telephone No. 49-89-2399-0

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE98/00563

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-11, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-18, filed with the letter of 20 May 1999 (20.05.1999),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig _____, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig 1/1, filed with the letter of 20 May 1999 (20.05.1999),
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

Citations

1. This international preliminary examination report refers to the following document:

D1: JP-A-06 315 027

Since document **D1**, which represents a prior art document under PCT Rule 64.1, is only available in Japanese, this international preliminary examination report uses for reference the subsequently published U.S. patent, **US-A-5 673 318**, which claims the same priority as **D1**. It is assumed that the content of document **US-A-5 673 318** is the same as that of **D1**.

2. Independent **Claims 1, 10 and 11** and dependent **Claims 3 and 12** do not meet the clarity requirement of PCT Article 6.

The following observations regarding the **novelty** (PCT Article 33(2)) and **inventive step** (PCT Article 33(3)) of independent **Claims 1, 10 and 11** and dependent **Claims 3 and 12** in this international preliminary examination report relate to the said

claims as understood taking into account the objections concerning lack of clarity under **Box VIII**.

3. This international patent application concerns a method for "forming" and for "checking a cryptographic commutative hash total" for digital data which is grouped into a plurality of data segments, as per the preamble to independent **Claims 1 and 2**.

4. The prior art closest to the subjects of independent **Claims 1 and 2** is considered to be document **D1**, which is cited in the international search report and likewise discloses a method as per the preamble to **Claims 1 and 2**.

In **D1**, each individual data segment is encoded using a cryptographic operation, for example by means of DES ("Data Encryption Standard"), and then a plurality of encoded data segments are subjected to an exclusive OR linking and shortening.

5. However, in contrast to the disclosure of **D1**, the present international patent application uses a two-stage security method in which a segment hash total is first formed for each data segment, a commutative hash total is then formed from these segment hash totals by commutative linking and finally this commutative hash total is encoded for security purposes by means of a cryptographic operation, thereby obtaining a cryptographic commutative hash total.

6. Although **D1** mentions replacing the "DES encoding"

procedure used by forming a "hash value" hash total, as is also used in the present international patent application, neither D1 nor any of the other international search report citations **discloses** or **suggests** the two-stage security method defined in independent **Claims 1 and 2**, which includes the formation of a hash total for each data segment and a subsequent cryptographic operation.

7.1 Independent **Claims 1 and 2** therefore meet the **novelty** and **inventive step** requirements of PCT Article 33(2) and (3).

7.2 The statement under 5.1 concerning the **novelty** and **inventive step** of independent **method Claims 1 and 2** likewise applies to the corresponding **device claims**, Claims **10 and 11**, which therefore likewise meet the requirements of PCT Article 33(2) and (3).

8. Dependent **Claims 3-9** and **12-18** are all directly or indirectly dependent on **Claims 1 and 2** or **10 and 11**, respectively, and therefore likewise meet the **novelty** and **inventive step** requirements of PCT Article 33(2) and (3).

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite document **D1** nor the relevant prior art disclosed therein.

2. Contrary to PCT Rule 5.1(a)(iii), the description is inconsistent with the claims.

3. Pursuant to PCT Rule 6.2(b), the technical features of the invention should be followed by reference signs in the claims. This requirement is not satisfied with regard to the reference sign ("**KP**") for the "cryptographic commutative hash total" in **Claims 1-3** and **10-12**.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Contrary to PCT Rule 6.4(a), **dependent Claims 3 and 12** ("method", or "arrangement for forming and checking...") do not contain a reference to the independent claims on which they depend, i.e. **Claims 1 and 2** ("method for forming...", "method for checking...") or **Claims 10 and 11** ("arrangement for forming...", "arrangement for checking..."), although they contain all the features of these independent claims.

2. Independent **Claims 1, 10 and 11** and dependent **Claims 3 and 12** do not meet the **clarity** requirements of PCT Article 6, since they all refer to a "method" or an "arrangement for forming or checking a ***commutative hash total***".

   However, taking into account all the features of the claims, in particular the feature whereby the "commutative hash total is secured by a cryptographic operation", it appears that the said claims refer rather to a "method" or an "arrangement for forming or checking a ***cryptographic commutative hash total***".

   This is not clear from the wording of the preamble to independent **Claims 1, 10 and 11** and dependent **Claims 3 and 12.**

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)
GR 97 P 1472 P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/DE98/00563	25/02/1998	14/04/1997

Internationale Patentklassification (IPK) oder nationale Klassifikation und IPK
H04L9/32

Anmelder
SIEMENS AKTIENGESELLSCHAFT et al.

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 6 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
26/08/1998	12.07.99

Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:

Europäisches Patentamt
D-80298 München
Tel. (+49-89) 2399-0 Tx: 523656 epmu d
Fax: (+49-89) 2399-4465

Bevollmächtigter Bediensteter

Möll, H-P

Tel. Nr. (+49-89) 2399 8243

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE98/00563

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-11	ursprüngliche Fassung				

Patentansprüche, Nr.:

1-18	eingegangen am	27/05/1999	mit Schreiben vom	20/05/1999	

Zeichnungen, Blätter:

1/1	eingegangen am	27/05/1999	mit Schreiben vom	20/05/1999	

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:
   ☐ Ansprüche, Nr.:
   ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-18
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	1-18
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-18
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Angeführte Unterlagen

1. In diesem Internationalen Vorläufigen Prüfungsbericht wird auf das folgende Dokument verwiesen:

   D1: JP-A-6 315 027

   Da das Dokument **D1**, welches ein Dokument des Standes der Technik gemäß Regel 64.1 PCT darstellt, nur in japanischer Sprache vorliegt, wird zur Referenzierung in diesem Internationalen Vorläufigen Prüfungsbericht das später veröffentlichte U.S. Patent **US-A-5 673 318** verwendet, welches die gleiche Priorität wie **D1** beansprucht. Es wird davon ausgegangen, dass das Dokument **US-A-5 673 318** inhaltlich mit **D1** übereinstimmt.

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Die unabhängigen **Ansprüche 1, 10 und 11** sowie die abhängigen **Ansprüche 3 und 12** genügen nicht dem Erfordernis des Artikels 6 PCT hinsichtlich Klarheit.

   Die folgenden Feststellungen über **Neuheit** (Artikel 33(2) PCT) sowie über **erfinderische Tätigkeit** (Artikel 33(3) PCT) der unabhängigen **Ansprüche 1, 10 und 11** sowie der abhängigen **Ansprüche 3 und 12** in diesem Internationalen Vorläufigen Prüfungsbericht, beziehen sich auf die genannten Ansprüche, wie sie unter Berücksichtigung der Klarheitseinwände unter **Punkt VIII** verstanden werden.

2. Diese Internationale Patentanmeldung betrifft ein Verfahren zur "Bildung" sowie zur "Überprüfung einer kryptographischen kommutativen Prüfsumme" für digitale Daten, die in mehrere Datensegmente gruppiert sind, gemäß Oberbegriff der unabhängigen **Ansprüche 1 und 2**.

3. Als nächstliegender Stand der Technik gegenüber den Gegenständen der unabhängigen **Ansprüche 1 und 2** wird das im Internationalen Recherchenbericht genannte Dokument **D1** erachtet, welches ebenfalls ein Verfahren gemäß Oberbegriff der **Ansprüche 1 und 2** offenbart.

   In **D1** wird jedes einzelne Datensegment unter Verwendung einer kryptographischen Operation, z.B. mittels DES ("Data Encryption Standard"), verschlüsselt und anschließend mehrere verschlüsselte Datensegmente einer EXKLUSIV-ODER-Verknüpfung sowie einer Verkürzung unterzogen.

4. Die vorliegende Internationale Patentanmeldung verwendet jedoch im Gegensatz zu der Offenbarung von **D1** eine zweistufige Sicherung, bei der für jedes Datensegment zuerst eine Segmentprüfsumme gebildet wird, anschließend aus diesen Segmentprüfsummen durch eine kommutative Verknüpfung eine kommutative Prüfsumme gebildet wird und zuletzt diese kommutative Prüfsumme mittels einer kryptographischen Operation zur Sicherung verschlüsselt wird und folglich eine kryptographische kommutative Prüfsumme erhalten wird.

5. Obwohl in **D1** ein Hinweis auf die Ersetzung der verwendeten "DES-Verschlüsselung" durch eine "Hashwert"-Prüfsummenbildung, wie sie auch in der vorliegenden Internationalen Patentanmeldung verwendet wird, zu finden ist, so wird jedoch die in den unabhängigen **Ansprüchen 1 und 2** definierte zweistufige Sicherung durch eine Prüfsummenbildung für jedes Datensegment und eine anschließende kryptographische Operation, durch **D1** oder ein anderes im Internationalen Recherchenbericht genanntes Dokument weder **offenbart** noch **nahegelegt**.

6.1 Die unabhängigen **Ansprüche 1 und 2** erfüllen daher die Erfordernisse des Artikels 33(2) und (3) PCT hinsichtlich **Neuheit** sowie **erfinderischer Tätigkeit**.

6.2 Die unter 5.1 getroffene Feststellung hinsichtlich **Neuheit** sowie **erfinderischer Tätigkeit** für die unabhängigen **Verfahrensansprüche 1 und 2**, gilt gleichermaßen für die korrespondierenden **Vorrichtungsansprüche 10 und 11**, die folglich ebenfalls die Erfordernisse des Artikels 33(2) und (3) PCT erfüllen.

7. Die abhängigen **Ansprüche 3-9**, sowie **12-18**, alle direkt oder indirekt von den **Ansprüchen 1 und 2**, bzw. **10 und 11** abhängig, erfüllen folglich ebenfalls die Erfordernisse des Artikels 33(2) und (3) PCT hinsichtlich **Neuheit** sowie **erfinderischer Tätigkeit**.

Zu Punkt VII
Bestimmte Mängel der internationalen Anmeldung

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in dem Dokument **D1** offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.

2. Im Widerspruch zur Regel 5.1(a)(iii) PCT steht die Beschreibung nicht in Einklang mit den Patentansprüchen.

3. Gemäß den Erfordernissen der Regel 6.2(b) PCT sind die technischen Merkmale der Erfindung in den Ansprüchen mit Referenzzeichen zu versehen.
Dieses Erfordernis ist hinsichtlich des Bezugszeichens ("**KP**") für die "kryptographische kommutative Prüfsumme" in den **Ansprüchen 1-3** sowie **10-12** nicht erfüllt.

Zu Punkt VIII
Bestimmte Bemerkungen zur internationalen Anmeldung

1. Im Widerspruch zur Regel 6.4(a) PCT sind die **abhängigen Ansprüche 3 und 12** ("Verfahren", bzw. "Anordnung zur Bildung und Überprüfung ... ") nicht mit einer Referenzierung auf die unabhängigen Ansprüche von denen Sie abhängen, d.h. **Anspruch 1 und 2** ("Verfahren zur Bildung ... ", "Verfahren zur Überprüfung ... "), bzw. **Anspruch 10 und 11** ("Anordnung zur Bildung ... ", "Anordnung zur Überprüfung ... "), versehen, obwohl sie alle Merkmale dieser unabhängigen Ansprüche enthalten.

2. Die unabhängigen **Ansprüche 1, 10 und 11** sowie die abhängigen **Ansprüche 3 und 12** erfüllen nicht die Erfordernisse des Artikels 6 PCT hinsichtlich **Klarheit**, da

sie sich alle auf ein "Verfahren", bzw. eine "Anordnung zur Bildung bzw. Überprüfung einer ***kommutativen* Prüfsumme**" beziehen.

Unter Berücksichtigung aller Merkmale der Ansprüche, insbesondere des Merkmals der "Sicherung der kommutativen Prüfsumme durch eine kryptographische Operation", erscheint es jedoch zuzutreffen, dass sich die genannten Ansprüche vielmehr auf ein "Verfahren", bzw. eine "Anordnung zur Bildung bzw. Überprüfung einer ***kryptographischen kommutativen* Prüfsumme**" beziehen.

Dies kommt durch die Formulierung des Oberbegriffs der unabhängigen **Ansprüche 1, 10 und 11** sowie der abhängigen **Ansprüche 3 und 12** nicht zum Ausdruck.

Neue Patentansprüche

1. Verfahren zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (PSi) die erste kommutative Prüfsumme (KP1) gebildet wird, und
c) bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

2. Verfahren zur Überprüfung einer vorgegebenen kryptographischen kommutativen Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, durch einen Rechner,
a) bei dem die kryptographische kommutative Prüfsumme einer inversen krytographischen Operation unterzogen wird zur Bildung einer ersten kryptographischen Prüfsumme (KP1),
b) bei dem für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,
c) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (PSj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
d) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

3. Verfahren zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,

b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (PSi) die erste kommutative Prüfsumme (KP1) gebildet wird,

c) bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird, wobei eine kryptographische kommutative Prüfsumme gebildet wird,

d) bei dem die kryptographische kommutative Prüfsumme (KP1) einer inversen krytographischen Operation unterzogen wird zur Bildung einer ersten rekontruierten kryptographischen Prüfsumme (KP1),

e) bei dem für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

f) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (PSj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

g) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten rekonstruierten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die Segmentprüfsummen (PSi, PSj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

6. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, bei dem die kommutative Verknüpfung (⊕) die Eigenschaft der Assoziativität aufweist.

8. Verfahren nach einem der Ansprüche 1 bis 7, bei dem digitale Daten geschützt werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

9. Verfahren nach einem der Ansprüche 1 bis 7, bei dem digitale Daten geschützt werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.

10. Anordnung zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (PSi) die erste kommutative Prüfsumme (KP1) gebildet wird, und
c) die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

11. Anordnung zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) die kryptographische kommutative Prüfsumme einer inversen krytographischen Operation unterzogen wird zur Bildung einer ersten kryptographischen Prüfsumme (KP1),
b) für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,

c) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (PSj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

d) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

12. Anordnung zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1... n) gruppiert sind,

mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß

a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,

b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird,

c) die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird, wobei eine kryptographische kommutative Prüfsumme gebildet wird,

d) die kryptographische kommutative Prüfsumme (KP1) einer inversen krytographischen Operation unterzogen wird zur Bildung einer ersten rekontruierten kryptographischen Prüfsumme (KP1),

e) für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

f) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

g) die zweite kommutative Prüfsumme (KP2) mit der ersten rekonstruierten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

13. Anordnung nach einem der Ansprüche 10 bis 12,

bei der die Recheneinheit derart eingerichtet ist, daß die Segmentprüfsummen (PSi, PSj) nach mindestens einer der folgenden Arten gebildet werden:

- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

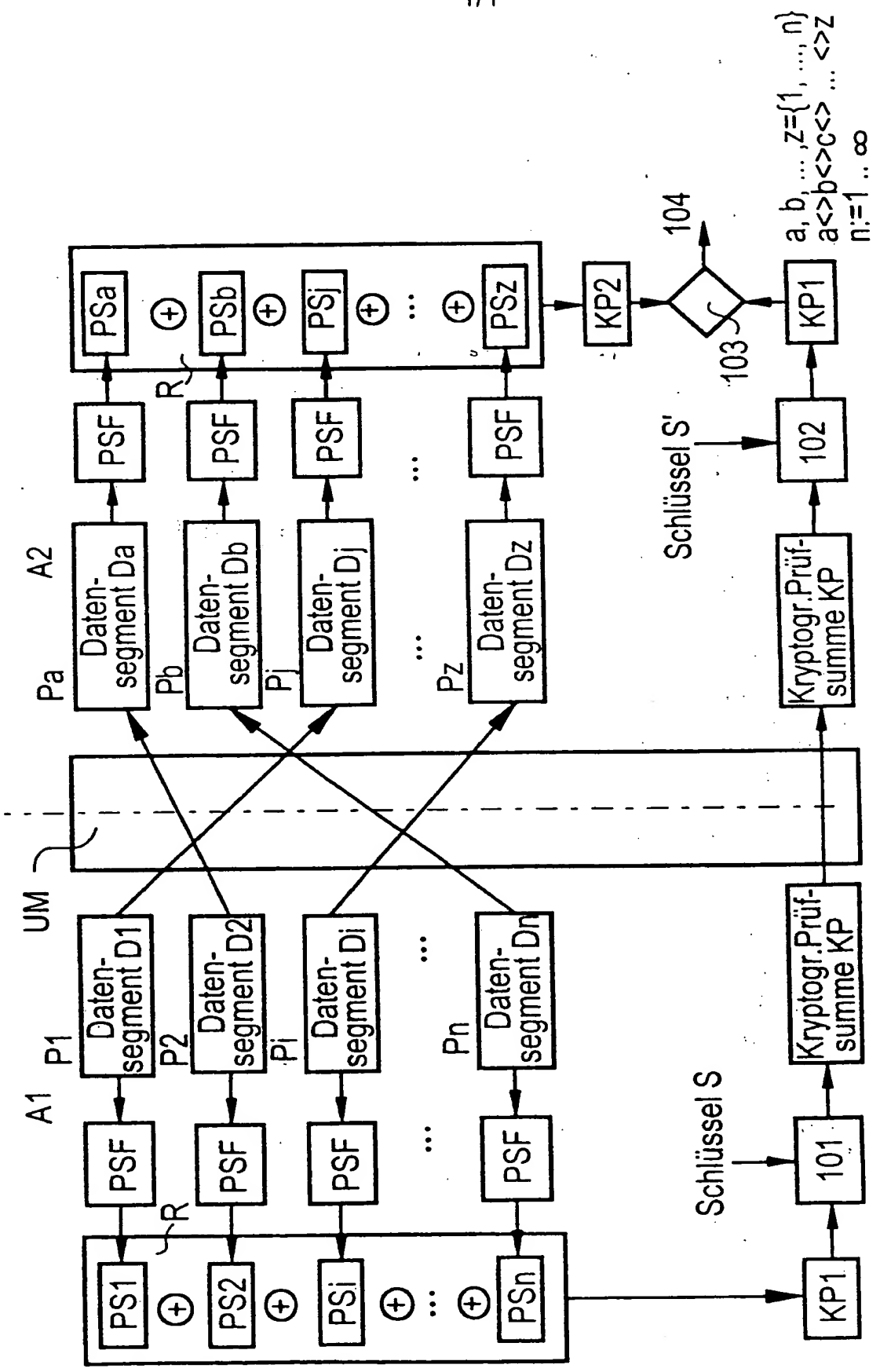
14. Anordnung nach einem der Ansprüche 10 bis 13, bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

15. Anordnung nach einem der Ansprüche 10 bis 13, bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

16. Anordnung nach einem der Ansprüche 10 bis 15, bei der die Recheneinheit derart eingerichtet ist, daß die kommutative Verknüpfung ($\oplus$) die Eigenschaft der Assoziativität aufweist.

17. Anordnung nach einem der Ansprüche 10 bis 16, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten geschützt werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

18. Anordnung nach einem der Ansprüche 10 bis 16, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten geschützt werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.


a, b, ..., z={1, ..., n}
a<>b<>c<> ... <>z
n:=1 .. 8
104
103
KP2
KP1
PSa
PSb
PSj
PSz
R
PSF
A2
Pa
Pb
Pj
Pz
Daten-segment Da
Daten-segment Db
Daten-segment Dj
Daten-segment Dz
Schlüssel S'
102
Kryptogr.Prüf-summe KP
UM
A1
P1
P2
Pi
Pn
Daten-segment D1
Daten-segment D2
Daten-segment Di
Daten-segment Dn
Schlüssel S
101
PS1
PS2
PSi
PSn

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro
INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04L 9/32 — A1

(11) Internationale Veröffentlichungsnummer: **WO 98/47264**

(43) Internationales Veröffentlichungsdatum: 22. Oktober 1998 (22.10.98)

(21) Internationales Aktenzeichen: PCT/DE98/00563

(22) Internationales Anmeldedatum: 25. Februar 1998 (25.02.98)

(30) Prioritätsdaten:
197 15 486.7 14. April 1997 (14.04.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HANCK, Martina [DE/DE]; Am Grenzweg 2, D–85635 Höhenkirchen (DE). HOFFMANN, Gerhard [DE/DE]; Gozbertstrasse 8/II, D–81547 München (DE). LUKAS, Klaus [DE/DE]; Niemöllerallee 6, D–81793 München (DE).

(81) Bestimmungsstaaten: AU, ID, JP, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

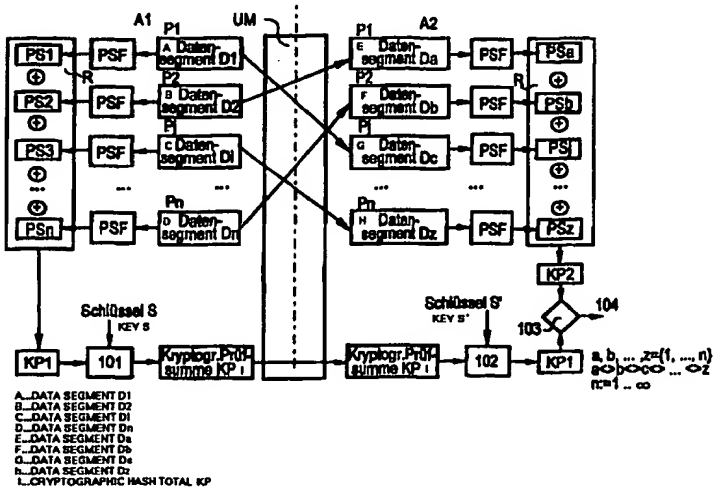
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND SYSTEM FOR PRODUCING AND CHECKING A HASH TOTAL FOR DIGITAL DATA GROUPED IN SEVERAL DATA SEGMENTS

(54) Bezeichnung: VERFAHREN UND ANORDNUNG ZUR BILDUNG UND ÜBERPRÜFUNG EINER PRÜFSUMME FÜR DIGITALE DATEN, DIE IN MEHRERE DATENSEGMENTE GRUPPIERT SIND

(57) Abstract

The invention relates to methods and systems for producing a hash total and checking a hash total for digital data, said data being grouped into data segments. According to this method, a hash total is produced for each data segment. The individual hash totals are combined to form a first commutative hash total using a commutative link. In order to check the first commutative hash total, another hash total is produced for each data segment and these hash totals are combined to form a second commutative hash total using a commutative link. The first commutative hash total and the second commutative hash total are then checked to make sure that they coincide.



(57) Zusammenfassung

Es werden Verfahren und Anordnungen zur Bildung einer Prüfsumme und zur Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, angegeben. Bei dem Verfahren wird für jedes Datensegment eine Prüfsumme gebildet. Die einzelnen Prüfsummen werden unter Verwendung einer kommutativen Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Zur Überprüfung der ersten kommutativen Prüfsumme wird für jedes Datensegment wiederum eine Prüfsumme gebildet und die Prüfsumme wiederum unter Verfahren einer kommutativen Verknüpfung zu einer zweiten kommutativen Prüfsumme verknüpft. Die erste kommutative Prüfsumme und die zweite kommutative Prüfsumme werden auf Übereinstimmung überprüft.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Beschreibung

Verfahren und Anordnung zur Bildung und Überprüfung einer Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind

Bei der digitalen Kommunikation, d.h. beim Austausch digitaler Daten ist es oftmals wünschenswert, die Übertragung der elektronischen Daten hinsichtlich verschiedenster Aspekte abzusichern.

Ein sehr bedeutender Aspekt ist der Schutz der zu übertragenden digitalen Daten gegen unerlaubte Modifikation, die sog. Sicherung der Integrität der Daten.

Aus [1] ist zum Schutz gegen unerlaubte Modifikation digitaler Daten die sog. kryptographische Prüfsumme bekannt, z.B. die digitale Signatur. Das in [1] beschriebene Verfahren basiert auf der Bildung eines Hashwertes aus den digitalen Nutzdaten und der anschließenden kryptographischen Bearbeitung des Hashwertes mit einem kryptographischen Schlüssel. Das Ergebnis ist eine kryptographische Prüfsumme. Zur Überprüfung der Integrität wird mit einem entsprechenden kryptographischen Schlüssel die inverse kryptographische Operation auf die gebildete Prüfsumme durchgeführt und das Ergebnis mit dem erneut aus den Nutzdaten berechneten Hashwert verglichen. Bei Übereinstimmung der ermittelten Hashwerte ist die Integrität der Nutzdaten gewährleistet.

Diese bisher übliche Vorgehensweise bedingt, daß die kompletten Nutzdaten auf Empfängerseite in identischer Reihenfolge, wie sie bei der Bildung des Hashwertes vorlagen, vorliegen müssen, da sonst die Hashwertbildung zu einem fehlerhaften Wert führt. Oftmals ist es jedoch bei der digitalen Kommunikation üblich, die zu übertragenden Nutzdaten aufgrund von Protokollrandbedingungen in kleinere Datensegmente, die auch als Datenpakete bezeichnet werden, zu unterteilen und zu

übertragen. Die Datensegmente sind oftmals nicht an eine definierte Reihenfolge gebunden oder ein definiertes sequentielles Eintreffen der Datensegmente kann nicht garantiert werden. Bei dem Verfahren aus [1] ist es also erforderlich, daß die kompletten Nutzdaten auf Empfängerseite, d.h. nach der Übertragung der Datensegmente wieder in der Reihenfolge, in der sie ursprünglich gesendet wurden, zusammengesetzt werden. Die zu übertragenden Daten können ausschließlich in dieser Reihenfolge verifiziert werden. Dies bedeutet jedoch oft einen erheblichen zusätzlichen Aufwand zur Flußkontrolle der Datensegmente, soweit dies überhaupt im Rahmen des verwendeten Protokolls möglich ist.

Aus [2] sind Grundlagen über kommutative Verknüpfungen bekannt. In [2] ist ferner eine allgemeine Definition für kommutative Verknüpfungen angegeben. Anschaulich ist unter einer kommutativen Verknüpfung eine Verknüpfung zu verstehen, bei der die Reihenfolge der Einzelverknüpfungen unwichtig ist und jede Reihenfolge der Einzelverknüpfung immer zu der gleichen Gesamtverknüpfung führt. Eine kommutative Verknüpfung kann beispielsweise eine EXOR-Verknüpfung, eine additive Verknüpfung oder auch eine multiplikative Verknüpfung sein.

Aus [3] sind ein Verfahren und eine Vorrichtung zur Erzeugung von Prüfkodesegmenten auf das Auftreten von Quelldaten hin und zur Ermittlung von Fehlern in den Quelldaten bekannt.

Somit liegt der Erfindung das Problem zugrunde, Verfahren und Anordnungen zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in mehrere Datensegmente gruppiert sind, anzugeben, bei der eine Flußkontrolle für die einzelnen Datensegmente nicht mehr erforderlich ist.

Das Problem wird durch das Verfahren gemäß Patentanspruch 1, durch das Verfahren gemäß Patentanspruch 2, durch das Verfahren gemäß Patentanspruch 3, durch die Anordnung gemäß Patent-

anspruch 11, durch die Anordnung gemäß Patentanspruch 12 sowie durch die Anordnung gemäß Patentanspruch 13, gelöst.

Bei dem Verfahren gemäß Patentanspruch 1 wird für digitale Daten, die in mehrere Datensegmente gruppiert sind, für jedes Datensegment eine erste Segmentprüfsumme gebildet. Die gebildeten ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft.

Bei dem Verfahren gemäß Patentanspruch 2 wird eine vorgegebene erste kommutative Prüfsumme, die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, überprüft. Dies erfolgt dadurch, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird und durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Bei dem Verfahren gemäß Patentanspruch 3 zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme für digitale Daten, die in Datensegmente gruppiert sind, wird für jedes Datensegment eine erste Segmentprüfsumme gebildet und die ersten Segmentprüfsummen werden durch eine kommutative Verknüpfung zu einer ersten kommutativen Prüfsumme verknüpft. Für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, werden zweite Segmentprüfsummen gebildet und durch kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet. Die zweite kommutative Prüfsumme und die erste kommutative Prüfsumme werden auf Übereinstimmung überprüft.

Die Anordnung gemäß Patentanspruch 11 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine Segmentprüfsumme gebildet wird, und daß durch eine kommutative Verknüpfung der Segmentprüfsummen die erste kommutative Prüfsumme gebildet wird.

Die Anordnung gemäß Patentanspruch 12 weist eine Recheneinheit auf, die derart eingerichtet ist, daß für jedes Datensegment eine zweite Segmentprüfsumme gebildet wird, durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen eine zweite kommutative Prüfsumme gebildet wird, und die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

Die Anordnung gemäß Patentanspruch 13 weist eine Recheneinheit auf, die derart eingerichtet ist, daß folgende Verfahrensschritte durchgeführt werden:

a) für jedes Datensegment wird eine Segmentprüfsumme gebildet,

b) durch eine kommutative Verknüpfung der Segmentprüfsummen wird die erste kommutative Prüfsumme gebildet,

c) für jedes Datensegment der digitalen Daten, denen die erste kommutative Prüfsumme zugeordnet ist, wird eine zweite Segmentprüfsumme gebildet,

d) durch eine kommutative Verknüpfung der zweiten Segmentprüfsummen wird eine zweite kommutative Prüfsumme gebildet, und

e) die zweite kommutative Prüfsumme wird mit der ersten kommutativen Prüfsumme auf Übereinstimmung überprüft.

Ein erheblicher Vorteil der Verfahren sowie der Anordnungen ist darin zu sehen, daß durch Verwendung einer kommutativen Verknüpfung für einzelne Prüfsummen der Datensegmente eine Flußkontrolle für die Reihenfolge der einzelnen Datensegmente nicht mehr erforderlich ist.

Es ist ferner nicht mehr erforderlich, die kompletten Nutzdaten wieder in der ursprünglichen Reihenfolge, in der die erste kommutative Prüfsumme gebildet wurde, zusammenzusetzen. Die Reihenfolge der einzelnen Datensegmente bei der Bildung der kommutativen Prüfsumme ist nicht mehr von Bedeutung.

Werden die digitalen Daten zwischen zwei Anordnungen übertragen, so ist ein weiterer Vorteil der Verfahren darin zu sehen, daß die Überprüfung der Integrität schon begonnen werden kann, bevor alle Datensegmente empfangen worden sind, da es nicht mehr erforderlich ist, die ursprüngliche Reihenfolge bei der Bildung der ersten Prüfsumme beizubehalten. Dies führt zu einer Zeitersparnis bei der Überprüfung der Integrität der Daten.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden.

Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Es ist vorteilhaft, die erste kommutative Prüfsumme unter Verwendung mindestens einer kryptographischen Operation kryptographisch abzusichern.

Durch diese Weiterbildung wird erreicht, daß die kryptographische Sicherheit der Daten erheblich erhöht wird. Eine kryptographische Operation in diesem Sinne ist beispielsweise die Verschlüsselung der ersten kommutativen Prüfsumme mit einem symmetrischen oder auch mit einem asymmetrischen Verschlüsselungsverfahren, wodurch eine kryptographische Prüfsumme gebildet wird. Auf Empfängerseite wird das inverse kryptographische Verfahren zu dem kryptographischen Verfahren durchgeführt, um die kryptographische Sicherheit zu gewährleisten.

Zur Bildung einer Prüfsumme, wie sie im Rahmen des Dokuments zu verstehen ist, sind verschiedene Möglichkeiten bekannt:
-eine Prüfsumme kann durch Bildung von Hashwerten für die einzelnen Datensegmente gebildet werden;

- die Prüfsummen können auch durch sog. zyklische Codes (Cyclic Redundancy Check, CRC) gebildet werden;
- es kann ferner eine kryptographische Einwegfunktion zur Bildung der Prüfsummen für die Datensegmente verwendet werden.

Die Verfahren können vorteilhaft in verschiedenen Anwendungsszenarien eingesetzt werden.

Die Verfahren können sowohl bei der Übertragung digitaler Daten zum Schutz vor Manipulation der Daten eingesetzt werden als auch bei der Archivierung digitaler Daten in einem Rechner, in dem die erste kommutative Prüfsumme gebildet wird, und zusammen mit den zu archivierenden Daten abgespeichert wird. Die erste kommutative Prüfsumme kann bei dem Laden der digitalen Daten aus dem Archivspeicher überprüft werden, um eine Manipulation der archivierten Daten zu erkennen.

Das Verfahren kann vorteilhaft für die Sicherung digitaler Daten verwendet werden, deren Datensegmente nicht an eine Reihenfolge gebunden sind. Beispiele für solche Datensegmente sind paketorientierte Kommunikationsprotokolle, z.B. Netzmanagementprotokolle wie das Simple Network Management Protocol (SNMP) oder das Common Management Information Protocol (CMIP).

Im weiteren wird ein Ausführungsbeispiel der Erfindung anhand einer Figur näher erläutert. Auch wenn das Ausführungsbeispiel im weiteren anhand des Simple-Network-Management-Protocols (SNMP) erläutert wird, so stellt dies keine Einschränkung der Verwendbarkeit des Verfahrens dar. Das Verfahren kann immer dann eingesetzt werden wenn es gilt, eine Integritätssicherung für digitale Daten zu gewährleisten, die in mehrere Datensegmente gruppiert sind.

Die Figur zeigt zwei Anordnungen, wobei von der ersten Anordnung Datensegmente zu der zweiten Anordnung übertragen werden.

In der Figur ist eine erste Rechneranordnung A1 symbolisch dargestellt, in der Datensegmente (Di, i = 1 .. n) gespeichert sind. Die Datensegmente Di bilden zusammen die digitalen Daten, die auch als Nutzdaten bezeichnet werden, für die es gilt, die Integrität zu gewährleisten.

Sowohl die erste Rechneranordnung A1 als auch eine im weiteren beschriebene zweite Rechneranordnung A2 enthalten jeweils eine Recheneinheit R, die derart eingerichtet ist, daß die im weiteren beschriebenen Verfahrensschritte durchgeführt werden.

In der ersten Anordnung A1 sind die Datensegmente Di an Positionen Pi innerhalb des gesamten Datenstroms angeordnet. Für jedes Datensegment Di wird eine erste Segmentprüfsumme PSi unter Verwendung einer Prüfsummenfunktion PSF. Die einzelnen ersten Segmentprüfsumme PSi werden durch eine kommutative Verknüpfung, wie sie in [2] definiert und beschrieben ist, zu einer ersten kommutativen Prüfsumme KP1 verknüpft. Die kommutative Verknüpfung zwischen den einzelnen Prüfsummen PSi sind in der Figur durch ein EXOR-Zeichen $\oplus$ symbolisch dargestellt.

Die erste kommutative Prüfsumme KP1 wird einem kryptographischen Verfahren, einem symmetrischen oder asymmetrischen Verfahren, unter Verwendung eines ersten kryptographischen Schlüssels S unterzogen (Schritt 101). Das Ergebnis der kryptographischen Operation ist eine kryptographische Prüfsumme KP.

Sowohl die Datensegmente Di als auch die kryptographische Prüfsumme KP werden über ein Übertragungsmedium, vorzugsweise eine Leitung oder auch eine logischen Verbindung, die in der

Fig. durch eine Kommunikationsverbindung UM symbolisch dargestellt ist, zu einer zweiten Anordnung A2 übertragen und dort empfangen.

Die sich überkreuzenden Pfeile der Datensegmente Di in der Figur deuten an, daß durch die Übertragung der Datensegmente Di diese in einer gegenüber der Reihenfolge in der ersten Anordnung A1 verschobenen Positionen Pj (j = a .. z) empfangen werden.

So wird ein Datensegment D2 an der ersten Position P1 in der zweiten Anordnung A2 als Datensegment Da empfangen. Das Datensegment D1 wird als Datensegment Dc in der zweiten Anordnung empfangen. Das Datensegment Dn wird als empfangenes Datensegment Db in der zweiten Anordnung A2 an der zweiten Position P2 empfangen.

Entsprechend dem verwendeten Verfahren wird entweder mit dem ersten kryptographischen Schlüssel S bei Verwendung eines symmetrischen Verschlüsselungsverfahrens die inverse kryptographische Operation auf die kryptographische Prüfsumme KP ausgeführt oder bei Verwendung eines asymmetrischen kryptographischen Verfahrens unter Verwendung eines zweiten kryptographischen Schlüssels S'.

Das Ergebnis der inversen kryptographischen Operation (Schritt 102) ist bei korrekter Verschlüsselung und Entschlüsselung wiederum die erste kommutative Prüfsumme KP1.

Diese wird in der zweiten Anordnung A2 gespeichert. Für den Vergleich der nunmehr in permutierter Reihenfolge, verglichen mit der ursprünglichen Reihenfolge bei der Bildung der ersten kommutativen Prüfsumme KP1 empfangenen Datensegmente Dj, werden wiederum unter Verwendung der gleichen Prüfsummenverfahren PSF zweite Segmentprüfsummen Psj für die empfangenen Datensegmente Dj gebildet.

Die sich ergebenden zweiten Prüfsummen PSj werden wiederum kommutativ miteinander verknüpft zu einer zweiten kommutativen Prüfsummen KP2.

In einem weiteren Schritt 103 wird überprüft, ob die erste kommutative Prüfsumme KP1 mit der zweiten kommutativen Prüfsumme KP2 übereinstimmt.

Ist dies der Fall, so ist die Integrität der Datensegmente Di und somit die Integrität der gesamten digitalen Daten gewährleistet (Schritt 104), wenn die verwendeten kryptographischen Verfahren bzw. die verwendeten Verfahren zur Prüfsummenbildung die entsprechende kryptographische Sicherheit gewährleisten.

Stimmen die erste kryptographische Prüfsumme KP1 und die zweite kryptographische Prüfsumme KP2 nicht miteinander überein, so würde die Integrität der Datensegmente Di verletzt und es wird eine Manipulation der Daten festgestellt und vorzugsweise einem Benutzer des Systems gemeldet.

Die Protokolldateneinheiten PDU (Protocol Data Units) sind in SNMP derart aufgebaut, daß in der Nutzdateninformation (sog. Variable Bindings) eine Liste von Objekten (Objektidentikatoren, OID/Value-Pairs) enthalten sein kann. Die Reihenfolge der Objekte innerhalb einer PDU ist dabei nicht festgelegt, so daß eine Permutation der Objekte bei der Übertragung der PDUs zwischen der ersten Anordnung A1 und der zweiten Anordnung A2 auftreten kann. Durch die Erfindung wird es nunmehr möglich, über alle Objekte einer SNMP-PDU eine einzige kryptographische Prüfsumme zu bilden, ohne daß die Reihenfolge der Objekte bzw. der PDUs berücksichtigt werden muß.

Im weiteren werden Alternativen zu dem oben beschriebenen Ausführungsbeispiel erläutert.

Das Verfahren zur Bildung der Prüfsumme PSF kann beispielsweise ein Verfahren zur Bildung von Hashwerten sein. Es kann aber auch Verfahren zur Bildung zyklischer Codes (Cyclic-Redundancy-Check, CRC) unter Verwendung rückgekoppelter Schieberegister eingesetzt werden. Auch können kryptographische Einwegfunktionen zur Bildung der Prüfsummen PSi bzw. PSj verwendet werden.

Ferner kann die kommutative Verknüpfung zusätzlich die Eigenschaft der Assoziativität aufweisen.

Sowohl das Verfahren zur Bildung der Prüfsumme als auch das Verfahren zur Überprüfung einer Prüfsumme können unabhängig voneinander durchgeführt werden. Es kann jedoch auch gemeinsam das Verfahren zur Bildung der Prüfsumme und das Verfahren zur Überprüfung der Prüfsumme durchgeführt werden.

Es ist ferner vorgesehen, keine Übertragung digitaler Daten vorzunehmen, sondern die digitalen Daten zu archivieren, d.h. in der ersten Anordnung A1 zu speichern, gemeinsam mit der ersten kommutativen Prüfsumme KP1. Bei der Wiederverwendung der archivierten Daten, d.h. beim Laden der Datensegmente Di aus dem Speicher der ersten Anordnung A1 wird dann das Verfahren zur Überprüfung der ersten kommutativen Prüfsumme KP1, wie es oben beschrieben wurde, durchgeführt. Somit können die erste Anordnung A1 und die zweite Anordnung A2 identisch sein.

Anschaulich kann die Erfindung darin gesehen werden, daß bei mehreren Datensegmenten, die insgesamt die zu schützenden Daten darstellen, für jedes Datensegment eine Prüfsumme gebildet wird und die einzelnen Prüfsummen der Datensegmente kommutativ miteinander verknüpft werden. Dadurch wird es möglich, eine Prüfsumme zu bilden und zu überprüfen, ohne daß die Reihenfolge der Datensegmente berücksichtigt werden muß.

Im Rahmen dieses Dokuments wurden folgende Veröffentlichungen zitiert:

[1] W. Stallings, Sicherheit in Netzwerk und Internet, Prentice Hall, ISBN 3-930436-29-9, S. 203-223, 1995

[2] K.-H. Kiyek und F. Schwarz, Mathmatik für Informatiker, Teubner Verlag, ISBN 3-519-03277-X, S. 11-13, 1989

[3] DE-OS 2 048 365

Patentansprüche

1. Verfahren zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird, und
b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird.

2. Verfahren zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,
b) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
c) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

3. Verfahren zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind, durch einen Rechner,
a) bei dem für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) bei dem durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird,
c) bei dem für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

d) bei dem durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) bei dem die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

6. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

7. Verfahren nach Anspruch 5,
bei dem die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

8. Verfahren nach einem der Ansprüche 1 bis 7,
bei dem die kommutative Verknüpfung (⊕) die Eigenschaft der Assoziativität aufweist.

9. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.

11. Anordnung zur Bildung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird, und
b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird.

12. Anordnung zur Überprüfung einer vorgegebenen ersten kommutativen Prüfsumme (KP1), die digitalen Daten zugeordnet ist, die in mehrere Datensegmente gruppiert sind,
mit einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Dj, j = a .. z) eine zweite Segmentprüfsumme (PSj) gebildet wird,
b) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und
c) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

13. Anordnung zur Bildung und Überprüfung einer ersten kommutativen Prüfsumme (KP1) für digitale Daten, die in mehrere Datensegmente (Di, i = 1 .. n) gruppiert sind,
mit mindestens einer Recheneinheit, die derart eingerichtet ist, daß
a) für jedes Datensegment (Di) eine Segmentprüfsumme (PSi) gebildet wird,
b) durch eine kommutative Verknüpfung (⊕) der Segmentprüfsummen (Psi) die erste kommutative Prüfsumme (KP1) gebildet wird,

c) für jedes Datensegment (Dj, j = a .. z) der digitalen Daten, denen die erste kommutative Prüfsumme (KP1) zugeordnet ist, eine zweite Segmentprüfsumme (PSj) gebildet wird,

d) durch eine kommutative Verknüpfung (⊕) der zweiten Segmentprüfsummen (Psj) eine zweite kommutative Prüfsumme (KP2) gebildet wird, und

e) die zweite kommutative Prüfsumme (KP2) mit der ersten kommutativen Prüfsumme (KP1) auf Übereinstimmung überprüft wird.

14. Anordnung nach einem der Ansprüche 11 bis 13,
bei der die Recheneinheit derart eingerichtet ist, daß die Segmentprüfsummen (Psi, Psj) nach mindestens einer der folgenden Arten gebildet werden:
- Hashwertbildung,
- Bildung von CRC-Codes,
- Verwendung mindestens einer kryptographischen Einwegfunktion.

15. Anordnung nach einem der Ansprüche 11 bis 14,
bei der die Recheneinheit derart eingerichtet ist, daß die erste kommutative Prüfsumme (KP1) unter Verwendung mindestens einer kryptographischen Operation kryptographisch gesichert wird.

16. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein symmetrisches kryptographisches Verfahren ist.

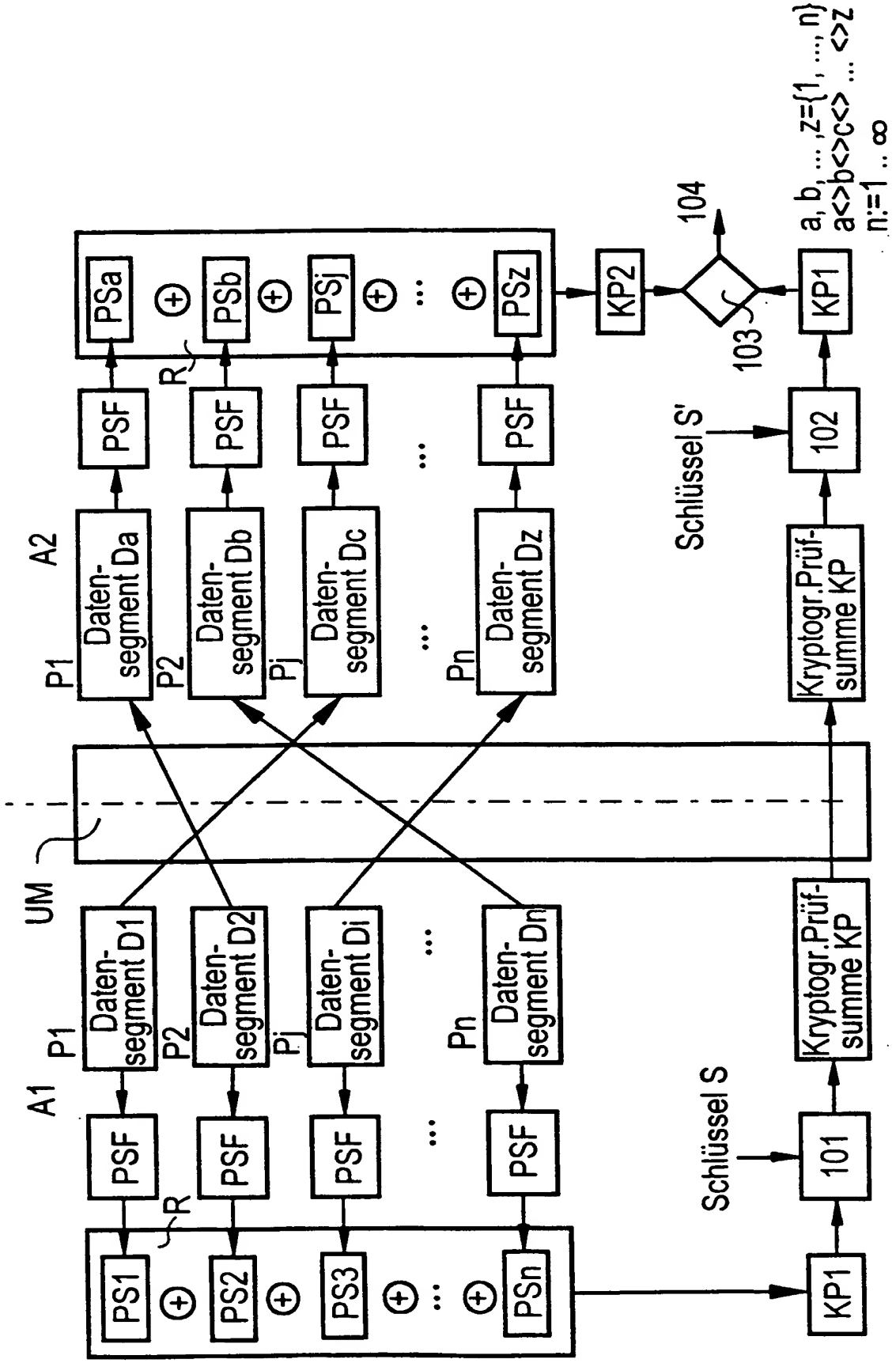
17. Anordnung nach Anspruch 15,
bei der die Recheneinheit derart eingerichtet ist, daß die kryptographische Operation ein asymmetrisches kryptographisches Verfahren ist.

18. Anordnung nach einem der Ansprüche 11 bis 17,

bei der die Recheneinheit derart eingerichtet ist, daß die kommutative Verknüpfung ($\oplus$) die Eigenschaft der Assoziativität aufweist.

19. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, deren Datensegmente (Di) nicht an eine Reihenfolge gebunden sind.

20. Anordnung nach einem der Ansprüche 11 bis 18, bei der die Recheneinheit derart eingerichtet ist, daß digitale Daten gesichert werden, die nach einem Netzmanagement-Protokoll verarbeitet werden.


A1
A2
UM
P1
P2
Pj
Pn
Daten-segment D1
Daten-segment D2
Daten-segment Di
Daten-segment Dn
Daten-segment Da
Daten-segment Db
Daten-segment Dc
Daten-segment Dz
PSF
R
PS1
PS2
PS3
PSn
PSa
PSb
PSj
PSz
KP1
KP2
Kryptogr.Prüf-summe KP
Schlüssel S
Schlüssel S'
101
102
103
104
a, b, ..., z={1, ..., n}
a<>b<>c<> ... <>z
n:=1 .. ∞

INTERNATIONAL SEARCH REPORT

International Application No
PCT/DE 98/00563

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 06 315 027 A (IBM) 8 November 1994	1-4, 11-14
A	see the whole document	6,16
P,X	& US 5 673 318 A (IBM) 30 September 1997	1-4, 11-14
A	see abstract see column 1, line 63 - column 2, line 30 see column 5, line 8 - column 6, line 22 see column 5, line 8 - column 6, line 22	6,16
X	EP 0 609 595 A (HEWLETT-PACKARD) 10 August 1994 see page 3, line 28 - line 35 see page 5, line 2 - line 37 see page 3, line 52 - page 4, line 12	1-4, 11-14

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 1998	14/08/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 654 920 A (FISCHER) 24 May 1995 see abstract see column 9, line 54 - column 10, line 5 see column 10, line 44 - line 58	1,5-8, 11,15-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[illegible]al Application No
PCT/DE 98/00563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 6315027 A	08-11-1994	US 5757913 A	26-05-1998
		US 5673318 A	30-09-1997
EP 609595 A	10-08-1994	JP 7015354 A	17-01-1995
		US 5778013 A	07-07-1998
EP 654920 A	24-05-1995	US 5475826 A	12-12-1995
		AU 3525397 A	11-12-1997
		AU 5778394 A	25-05-1995
		CA 2120678 A	20-05-1995
		JP 8083046 A	26-03-1996
		US 5694569 A	02-12-1997

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/00563

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	JP 06 315 027 A (IBM) 8. November 1994	1-4, 11-14
A	siehe das ganze Dokument	6,16
P,X	& US 5 673 318 A (IBM) 30. September 1997	1-4, 11-14
A	siehe Zusammenfassung siehe Spalte 1, Zeile 63 - Spalte 2, Zeile 30 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22	6,16

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 1998	14/08/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 609 595 A (HEWLETT-PACKARD) 10. August 1994 siehe Seite 3, Zeile 28 - Zeile 35 siehe Seite 5, Zeile 2 - Zeile 37 siehe Seite 3, Zeile 52 - Seite 4, Zeile 12	1-4, 11-14
A	EP 0 654 920 A (FISCHER) 24. Mai 1995 siehe Zusammenfassung siehe Spalte 9, Zeile 54 - Spalte 10, Zeile 5 siehe Spalte 10, Zeile 44 - Zeile 58	1,5-8, 11,15-18

INTERNATIONALER [redacted]CHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inte[redacted]onales Aktenzeichen
PCT/DE 98/00563

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
JP 6315027 A	08-11-1994	US 5757913 A	26-05-1998
		US 5673318 A	30-09-1997
EP 609595 A	10-08-1994	JP 7015354 A	17-01-1995
		US 5778013 A	07-07-1998
EP 654920 A	24-05-1995	US 5475826 A	12-12-1995
		AU 3525397 A	11-12-1997
		AU 5778394 A	25-05-1995
		CA 2120678 A	20-05-1995
		JP 8083046 A	26-03-1996
		US 5694569 A	02-12-1997

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
GR 97 P 1472 P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/DE 98/ 00563	25/02/1998	14/04/1997
Anmelder		
SIEMENS AKTIENGESELLSCHAFT et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. [ ] **Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen** (siehe Feld I).

2. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

3. [ ] In der internationalen Anmeldung ist **ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz** offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
   - [ ] das zusammen mit der internationalen Anmeldung eingereicht wurde.
   - [ ] das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde.
     - [ ] dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
   - [ ] das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.

4. Hinsichtlich der **Bezeichnung der Erfindung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt.

5. Hinsichtlich der **Zusammenfassung**
   - [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.
   - [ ] wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen:
   Abb. Nr. 1
   - [ ] wie vom Anmelder vorgeschlagen
   - [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
   - [ ] weil diese Abbildung die Erfindung besser kennzeichnet.
   - [ ] keine der Abb.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 98/00563

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04L9/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	JP 06 315 027 A (IBM) 8. November 1994	1-4, 11-14
A	siehe das ganze Dokument	6,16
P,X	& US 5 673 318 A (IBM) 30. September 1997	1-4, 11-14
A	siehe Zusammenfassung siehe Spalte 1, Zeile 63 - Spalte 2, Zeile 30 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22 siehe Spalte 5, Zeile 8 - Spalte 6, Zeile 22	6,16

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 1998	14/08/1998

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

2

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 609 595 A (HEWLETT-PACKARD) 10. August 1994 siehe Seite 3, Zeile 28 - Zeile 35 siehe Seite 5, Zeile 2 - Zeile 37 siehe Seite 3, Zeile 52 - Seite 4, Zeile 12 ---	1-4, 11-14
A	EP 0 654 920 A (FISCHER) 24. Mai 1995 siehe Zusammenfassung siehe Spalte 9, Zeile 54 - Spalte 10, Zeile 5 siehe Spalte 10, Zeile 44 - Zeile 58 -----	1,5-8, 11,15-18

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/DE 98/00563

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 6315027 A	08-11-1994	US 5757913 A	26-05-1998
		US 5673318 A	30-09-1997
EP 609595 A	10-08-1994	JP 7015354 A	17-01-1995
		US 5778013 A	07-07-1998
EP 654920 A	24-05-1995	US 5475826 A	12-12-1995
		AU 3525397 A	11-12-1997
		AU 5778394 A	25-05-1995
		CA 2120678 A	20-05-1995
		JP 8083046 A	26-03-1996
		US 5694569 A	02-12-1997

PA. JT COOPERATION TREAT\

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing: 22 October 1998 (22.10.98)	
International application No.: PCT/DE98/00563	Applicant's or agent's file reference: GR 97 P 1472 P
International filing date: 25 February 1998 (25.02.98)	Priority date: 14 April 1997 (14.04.97)
Applicant: HANCK, Martina et al	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

26 August 1998 (26.08.98)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

Replaced by Article 34 Amdt

Patent Claims

1. Method for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di), and

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi).

2. Method for checking a predetermined first commutative checksum (KP1) which is allocated to digital data which are grouped into a number of data segments, by a computer,

a) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z),

b) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (Psj), and

c) in which the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

3. Method for forming and checking a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by a computer,

a) in which a segment checksum (PSi) is formed for each data segment (Di),

b) in which the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (PSi),

c) in which a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,

d) in which a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (Psj), and

e) in which the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

4. Method according to one of Claims 1 to 3, in which the segment checksums (Psi, Psj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

5. Method according to one of Claims 1 to 4, in which the first commutative checksum (KP1) is cryptographically protected by using at least one cryptographic operation.

6. Method according to Claim 5, in which the cryptographic operation is a symmetric cryptographic method.

7. Method according to Claim 5, in which the cryptographic operation is an asymmetric cryptographic method.

8. Method according to one of Claims 1 to 7, in which the commutative operation (⊕) exhibits the property of associativity.

9. Method according to one of Claims 1 to 8, in which digital data are protected, the data segments (Di) of which are not tied to an order.

10. Method according to one of Claims 1 to 8, in which digital data are protected which are processed in accordance with a network management protocol.

11. Arrangement for forming a first commutative checksum (KP1) for digital data which are grouped into a number of data segments (Di, i = 1 .. n), by means of an arithmetic and logic unit which is arranged in such a manner that

a) a segment checksum (PSi) is formed for each data segment (Di), and

b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksum (Psi).

12. Arrangement for checking a predetermined first commutative checksum (KP1) which is allocated to digital data which are grouped into a number of data segments, by means of an arithmetic and logic unit which is arranged in such a manner that

a) a second segment checksum (Psj) is formed for each data segment (Dj, j = a .. z),

b) a second commutative checksum (KP2) formed by a commutative operation (⊕) on the second segment checksum (Psj), and

c) the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

13. Arrangement for forming and checking a first commutative checksum (KP1) for digital data which is grouped into a number of data segments (Di, i = 1 .. n), by means of at least one arithmetic and logic unit which is arranged in such a manner that

a) a segment checksum (PSi) is formed for each data segment (Di),

b) the first commutative checksum (KP1) is formed by a commutative operation (⊕) on the segment checksums (Psi),

c) a second segment checksum (PSj) is formed for each data segment (Dj, j = a .. z) of the digital data to which the first commutative checksum (KP1) is allocated,

d) a second commutative checksum (KP2) is formed by a commutative operation (⊕) on the second segment checksums (Psj), and

e) the second commutative checksum (KP2) is checked for a match with the first commutative checksum (KP1).

14. Arrangement according to one of Claims 11 to 13, in which the arithmetic and logic unit is arranged in such a manner that the segment checksums (Psi, Psj) are formed in accordance with at least one of the following types:

- forming a hashing value,
- forming CRC codes,
- using at least one cryptographic one-way function.

15. Arrangement according to one of Claims 11 to 14, in which the arithmetic and logic unit is arranged in such a manner that the first commutative checksum (KP1) is cryptographically protected using at least one cryptographic operation.

16. Arrangement according to Claim 15, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is a symmetric cryptographic method.

17. Arrangement according to Claim 15, in which the arithmetic and logic unit is arranged in such a manner that the cryptographic operation is an asymmetric cryptographic method.

18. Arrangement according to one of Claims 11 to 17,

in which the arithmetic and logic unit is arranged in such a manner that the commutative operation ($\oplus$) exhibits the property of associativity.

19. Arrangement according to one of Claims 11 to 18, in which the arithmetic and logic unit is set up in such a manner that the digital data are protected, the data segments (Di) of which are not tied to an order.

20. Arrangement according to one of Claims 11 to 18, in which the arithmetic and logic unit is arranged in such a manner that the digital data are protected which are processed in accordance with a network management protocol.